REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1, 3-5, 7-9 and 11-18 are pending in the application. No claim amendments are presented, thus no new matter is added.

In the Office Action, Claims 1, 3-5, 7-9 and 11-18 are rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. 6,248,946 to Dwek in view of U.S. Pub. 2001/0051996 to Cooper et al. (herein, Cooper).

In response to the above noted rejection under 35 U.S.C. § 103, Applicant respectfully submits that independent Claims 1, 9 and 13 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1, for example, recites, in part, a user authentication method for an authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

> registering, at an authentication server, unique identification information corresponding to a mobile information terminal, ***the unique information including*** a manufacturer code identifying the manufacturer of the mobile information terminal ***and*** an identification code unique to the mobile information terminal ...
>
> receiving, at the authentication server from said mobile information terminal, ***the unique identification information as encrypted by a predetermined encryption algorithm*** by a Web browser installed on said mobile information terminal ...

Independent Claims 9 and 13, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 9 and 13.

In rejecting Claim 1, p. 4 of the Office Action concedes that Dwek fails to teach or suggest that "the unique information corresponds to a mobile information terminal and includes a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal and wherein that information is encrypted ..." In an attempt to remedy this deficiency, the Office Action relies on Cooper. Applicant respectfully traverses this rejection, as Cooper fails to teach or suggest the claimed features for which it is asserted as a secondary reference under 35 U.S.C. § 103.

In rejecting the features directed to the contents of the "unique information", the Office Action relies on paragraphs [0159] – [0161] of Cooper. This cited portion of Cooper describes that each device includes a (e.g., a single) unique ID, which may be used, for example, to calculate the necessary values to build key and certificate files for creating encryption keys and digital certificates. Cooper describes that this unique ID may be, for example, a sequential number, a Universally Unique ID (UUID) or a Globally Unique ID (GUID), a MAC Address of a network interface card, or a static IP address.

Cooper, therefore, does appear to describe that a single unique ID may be associated with a device, but describes that this ID may be used to calculate values necessary to build files used to encrypt data. Thus, Cooper does not describe that the unique ID itself is actually encrypted, as required by independent Claim 1.

Moreover, Claim 1 requires that the "unique information" include "a manufacturer code identifying the manufacturer of the mobile information terminal ***and*** an identification code unique to the mobile information terminal". Cooper, on the other hand, fails to teach or suggest that a plurality of unique identification codes are associated with a device whatsoever, much less that the plurality of codes are encrypted by the device as collective "unique information", as required by independent Claim 1.

Further, p. 4 of the Office Action relies, *inter alia*, on paragraph [0058] of Cooper, noting that this cited portion of Cooper uses the term "encrypted". However, this cited portion of Cooper describes a content distribution environment, in which transactions containing sensitive data may have the appropriate fields encrypted prior to storing, and by encrypting the content data as it is transferred, a VPN may be established between the content and the user.

Thus, this cited portion of Cooper is directed to encrypting content, and not encrypting "unique information" that includes both "a manufacturer code identifying the manufacturer of the mobile information terminal ***and*** an identification code unique to the mobile information terminal", as recited in independent Claim 1.

Therefore, even if Dwek were combined with Cooper, the combination of these references fail to teach or suggest the above differentiated features recited in independent Claim 1.

Accordingly, for at least the reasons discussed above, Applicant respectfully requests that the rejection of Claims 1, 3-5, 7-9 and 11-18 under 35 U.S.C. § 103 be withdrawn.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-5, 7-9 and 11-18 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)